updating a so-called subscriber identification module (SIM) in mobile stations. The SIM stores data for controlling the mobile stations and for access to the services of the mobile radio network. The data stored in the SIM can be changed, i.e., updated, over the radio air interface. However, a method for personalizing a SIM over the air interface is not described.

WO-A-97/14258 also describes a method and a device for programming a mobile station via an air interface. Optionally, programs stored in the mobile station are here replaced or additional data are transmitted via the air interface. The method described herein also permits an initial activation of the mobile station via the air interface, but not a personalization of a subscriber identification module.

WO-A-93/07697 relates to a method for personalizing an active so-called SIM card. The SIM card is here completely personalized in an authorized terminal equipment which is connected via an encrypted communication line with a the central computer of the mobile radio network. However, a personalization of the chip card when the subscriber first logs on to the mobile radio network, is also neither taught nor suggested by this reference. - -

N.E. Page 2, please delete line 24-27 and

Page 3 delete entirely and insert instead

- - **SUMMARY OF THE INVENTION**

To solve the object, the invention propose that the personalization of the chip is performed when the subscriber logs on to the subscriber network for the first time, wherein the following process steps are carried out in that in a first process step, the chip manufacturer obtains the ICCID and the IMSI from a number pool, the chip itself derives an initial key Ki_1 from a key K1 which is known to and entered into the chip by the chip manufacturer, while PIN and PUK are set to a default value, in a second process step, an entry is made in the authentication center (AC) and the home location register (HLR) as soon as a subscriber has entered into a contract with the network operator, in a third process step, the authentication center (AC) also derives the initial first key Ki_1, in a fourth process step, the network sets the conditions so that during logon to the network, a connection is established from the chip to the security center of the network operator (SC), in a fifth process step, the connection is routed from the chip to the SC during the first logon, in a sixth process step, a new second secret key Ki_2 and, optionally, a PUK is negotiated with the chip or generated in the security center (SC) and transmitted to the chip, in a seventh process step, the conditions of the fourth process step are disabled again.

Further, a chip is provided wherein in the memory range of the chip there are stored at least one subscriber identification number IMSI and a card number ICCID as well as for the purpose of personalization an additional secret key Ki and, optionally, additional data, wherein for pre-personalizing the chip there are further stored initial card-related data, namely a first secret key Ki_1 and, optionally, additional data, such as PIN and PUK, characterized in that

the chip in the terminal equipment is Toolkit-enabled and includes means for communicating with a security center (SC) and negotiating a key.

The technical teachings according to the invention attains the following advantages: Elimination of a central personalization at the network operator; Issuance of a large number of GSM chips without producing a static load at the network operator; Reuse of "used" GSM chips; Regular change of the secret key Ki while used by the customer.

With the proposed method, the device manufacturer/chip manufacturer applies initial data associated with the card to the chip, which could be referred to as pre-personalization. The network operator himself performs the actual personalization at a later time and only for those customers who enter into a contract with the network operator.

The pre-personalization does not yet produce a static load at the network operator. The method therefore makes it possible to distribute "millions" of GSM chips, for example in each and every automobile, in each laptop computer or in each alarm system, and to subsequently "activate" only the chips of those customers who enter into a contract.

It is also possible to reuse cards if a customer terminates his contract (for example, if he sells his automobile).

In particular, in the case of the network operator D1, the dealer could release returned cards again for another customer. The network operator therefore eliminates the personalization of cards in the terminal equipment replacement business.

On page 9, on line 11, please insert:

-- **BRIEF DESCRIPTION OF THE DRAWINGS** --;

On page 9, line 20, please insert:

**--DETAILED DESCRIPTION OF THE PRESENTLY PREFERRED EMBODIMENTS** --;

On page 15, delete "SUMMARY" and insert --ABSTRACT- -;

REMARKS

This Preliminary Amendment has been made to add/replace the substitute pages from the PCT International application into the national phase prosecution and to prosecute the claims that were submitted as replacement claims. Such claims have been rewritten to conform to the US prosecution standards. No new matter was added.